在ISE 3.2中配置被动ID会话的授权流

目录

简介

本文档介绍如何配置被动ID事件的授权规则以将SGT分配到会话。

背景信息

被动身份服务（被动ID）不会直接对用户进行身份验证，而是从外部身份验证服务器(例如Active Directory(AD)，即提供商收集用户身份和IP地址，然后与用户共享该信息。

ISE 3.2引入了一项新功能，允许您配置授权策略，根据Active Directory组成员资格向用户分配安全组标记(SGT)。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ISE 3.X
- 与任何提供商的被动ID集成
- Active Directory(AD)管理
- 分段(Trustsec)
- PxGrid（平台交换网格）

使用的组件

- 身份服务引擎(ISE)软件版本3.2
- Microsoft Active Directory
- 系统日志

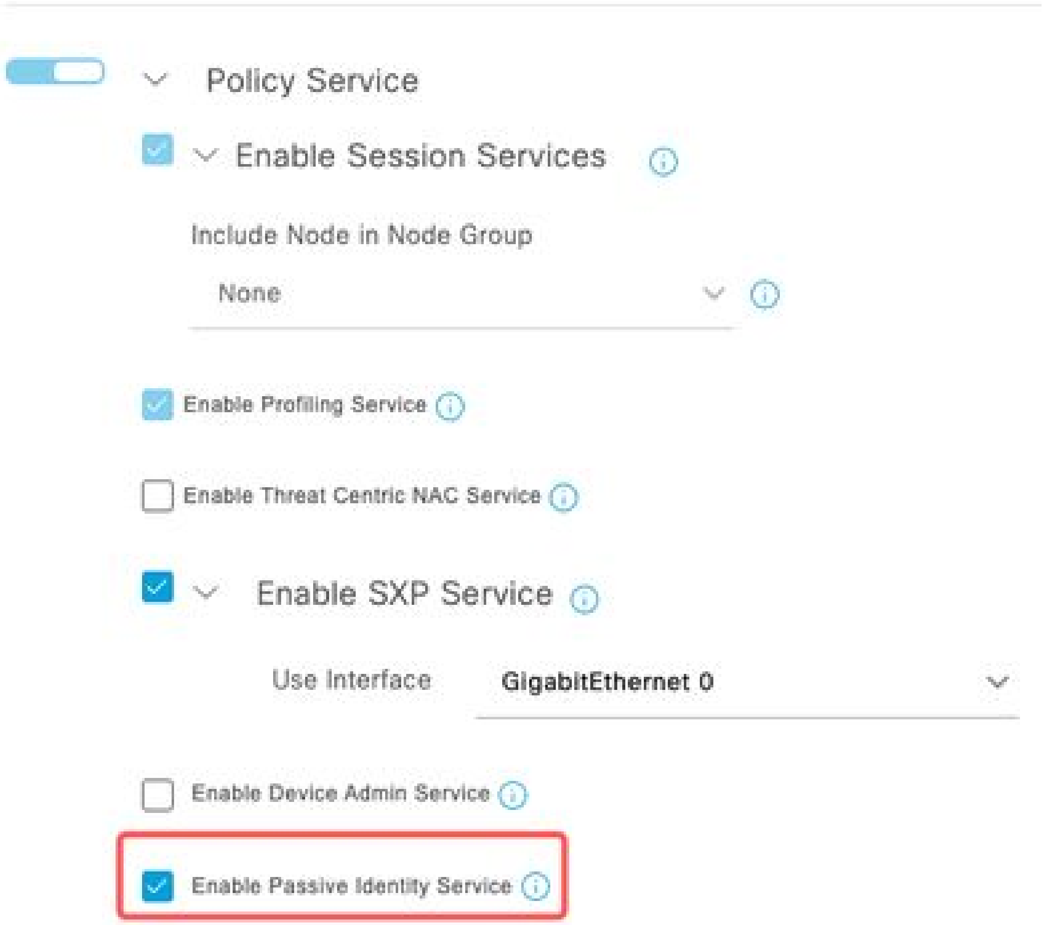
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

步骤1:启用ISE服务。

1. 在ISE上，导航到Administration > **Deployment**，选择ISE节点，然后单击**Edit**，启用**Policy Service**，然后选择**Enable Passive Identity Service**。可选，如果需要通过每个SXP和PxGrid发布被动ID会话，则可以启用SXP和PxGrid。Click Save.

   警告：由API提供程序进行身份验证的PassiveID登录用户的SGT详细信息无法发布到SXP。但是，这些用户的SGT详细信息可以通过pxGrid和pxGrid Cloud发布。



Policy Service

☑ Enable Session Services

Include Node in Node Group

None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

☑ Enable SXP Service

Use Interface GigabitEthernet 0

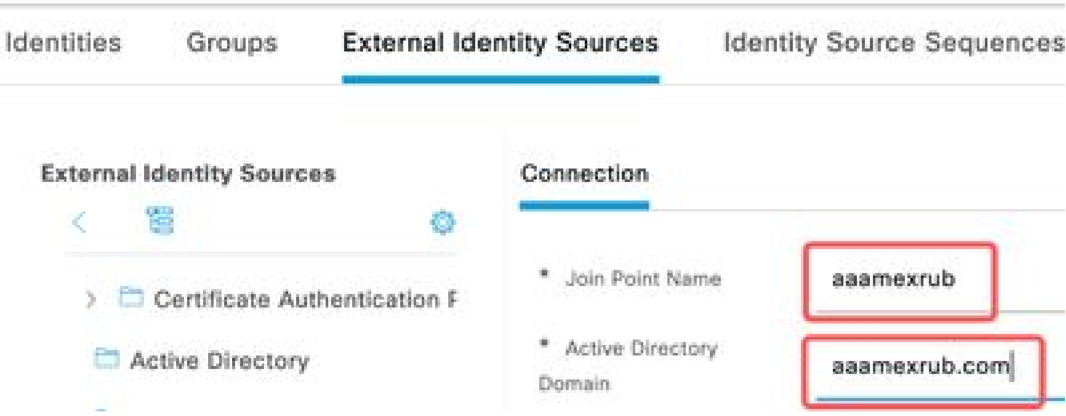
□ Enable Device Admin Service

☑ Enable Passive Identity Service

服务已启用

第二步：配置Active Directory。

1. 导航到Administration > **Identity Management** > **External Identity Sources**，然后选择**Active directory**，然后单击**Add**按钮。
2. 输入**加入点名称和Active Directory域**。单击“Submit”。

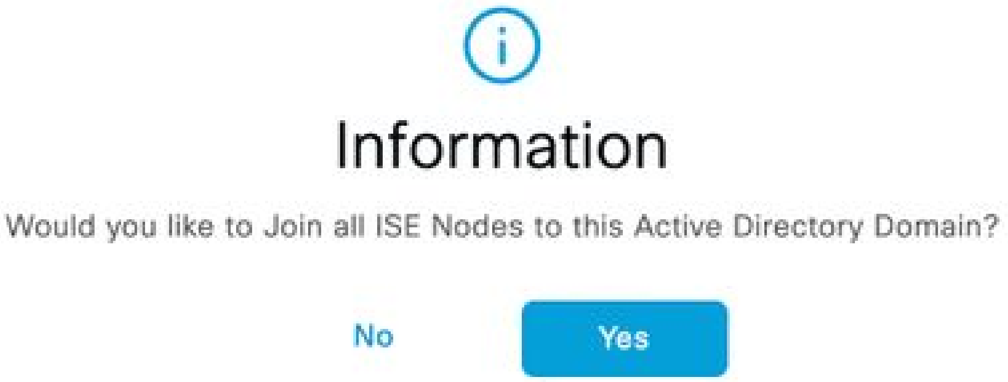

Identities
Groups
External Identity Sources
Identity Source Sequences
External Identity Sources
Certificate Authentication F
Active Directory
Connection

* Join Point Name: aaamexrub

* Active Directory Domain: aaamexrub.com

添加Active Directory

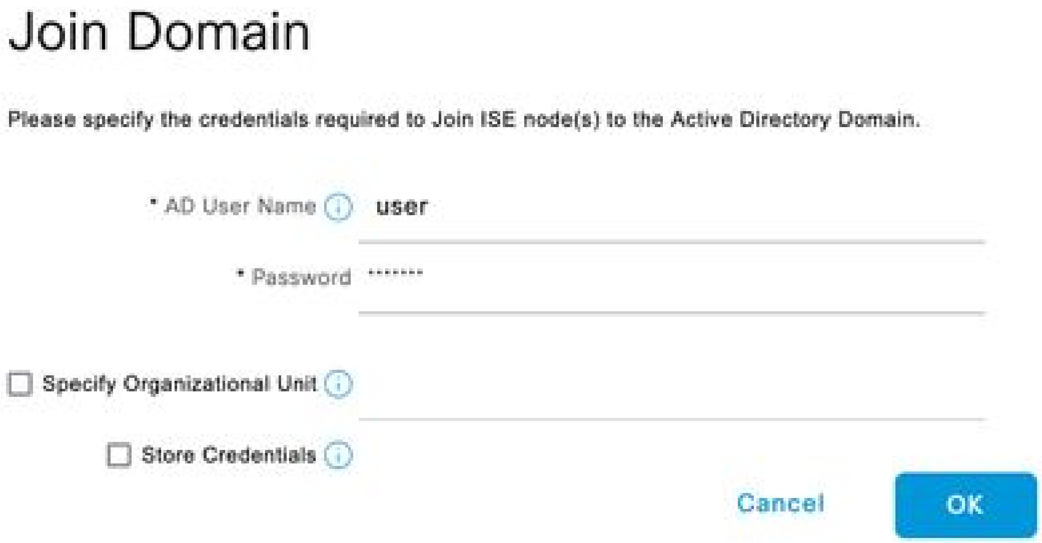
3.弹出窗口会将ISE加入AD。单击 Yes。输入用户名和口令。Click OK.



Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

继续加入



Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name: user

* Password: *******

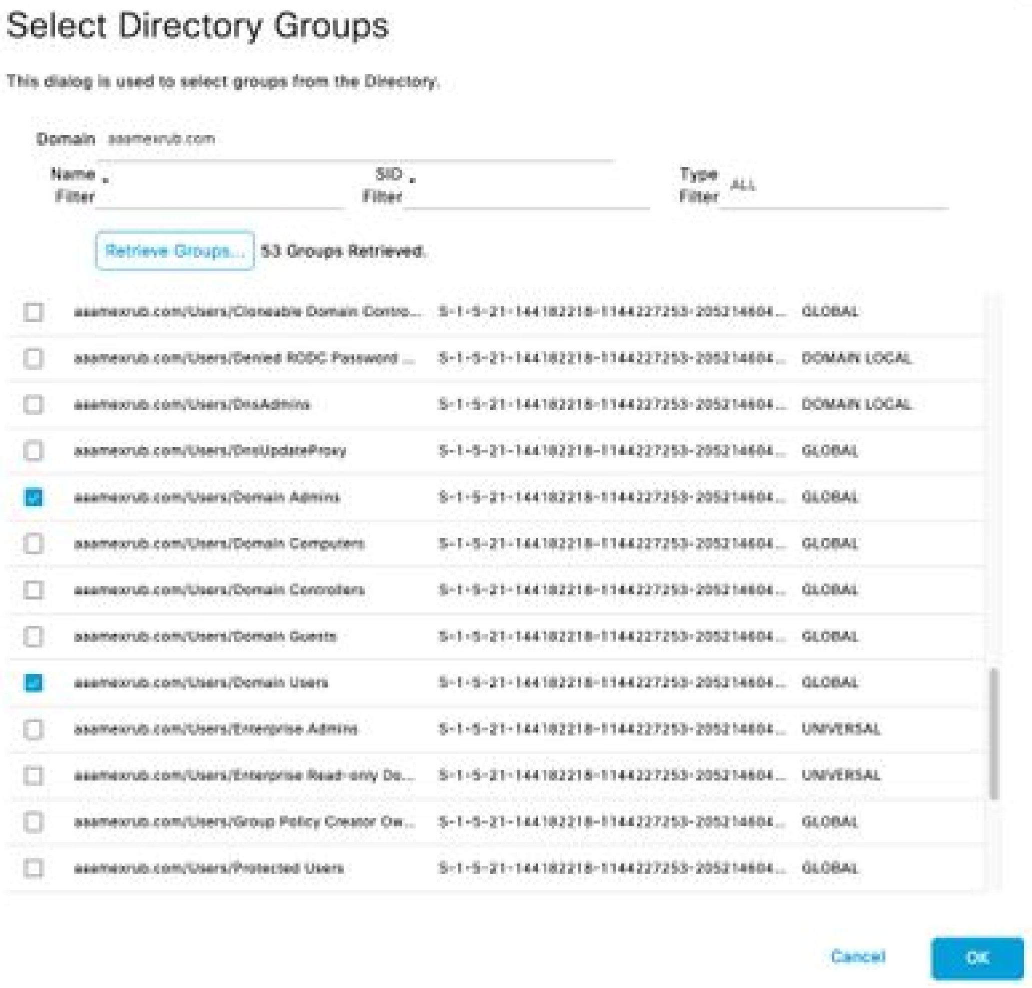
□ Specify Organizational Unit

□ Store Credentials

ISE

加入Active Directory

4.检索AD组导航到**Groups**，单击**Add**，然后单击**Retrieve Groups**，然后选择所有感兴趣的组，然后单击**OK**。



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain aaamexrub.com

Name Filter *

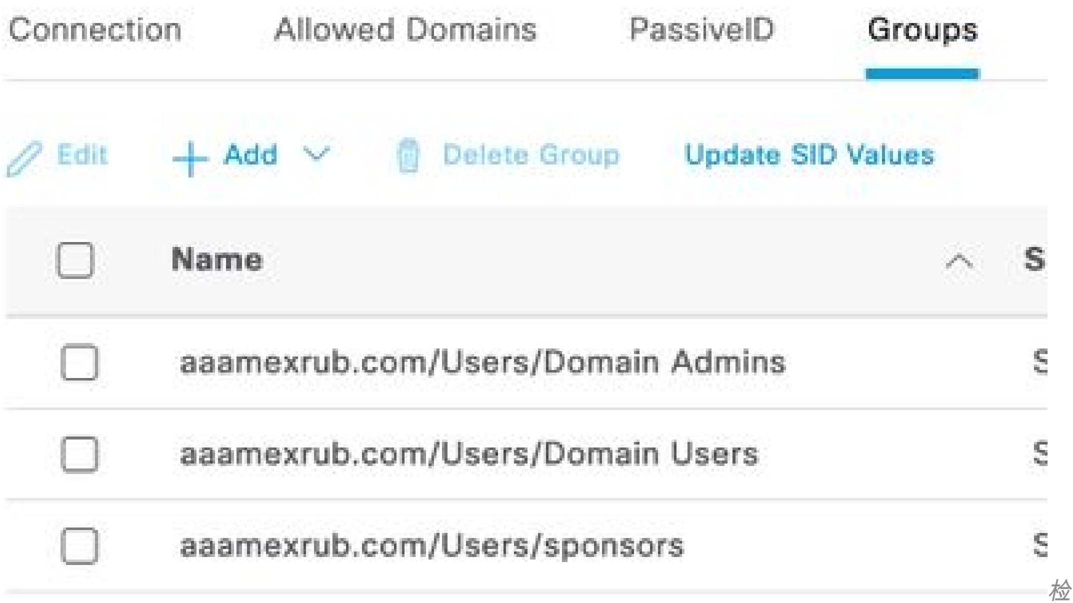
SID Filter *

Type Filter ALL

53 Groups Retrieved.

□	aaamexrub.com/Users/Cloneable Domain Contro...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Denied RODC Password ...	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
□	aaamexrub.com/Users/DnsAdmins	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
□	aaamexrub.com/Users/DnsUpdateProxy	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
☑	aaamexrub.com/Users/Domain Admins	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Domain Computers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Domain Controllers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Domain Guests	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
☑	aaamexrub.com/Users/Domain Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Enterprise Admins	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
□	aaamexrub.com/Users/Enterprise Read-only Do...	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
□	aaamexrub.com/Users/Group Policy Creator Ow...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Protected Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL

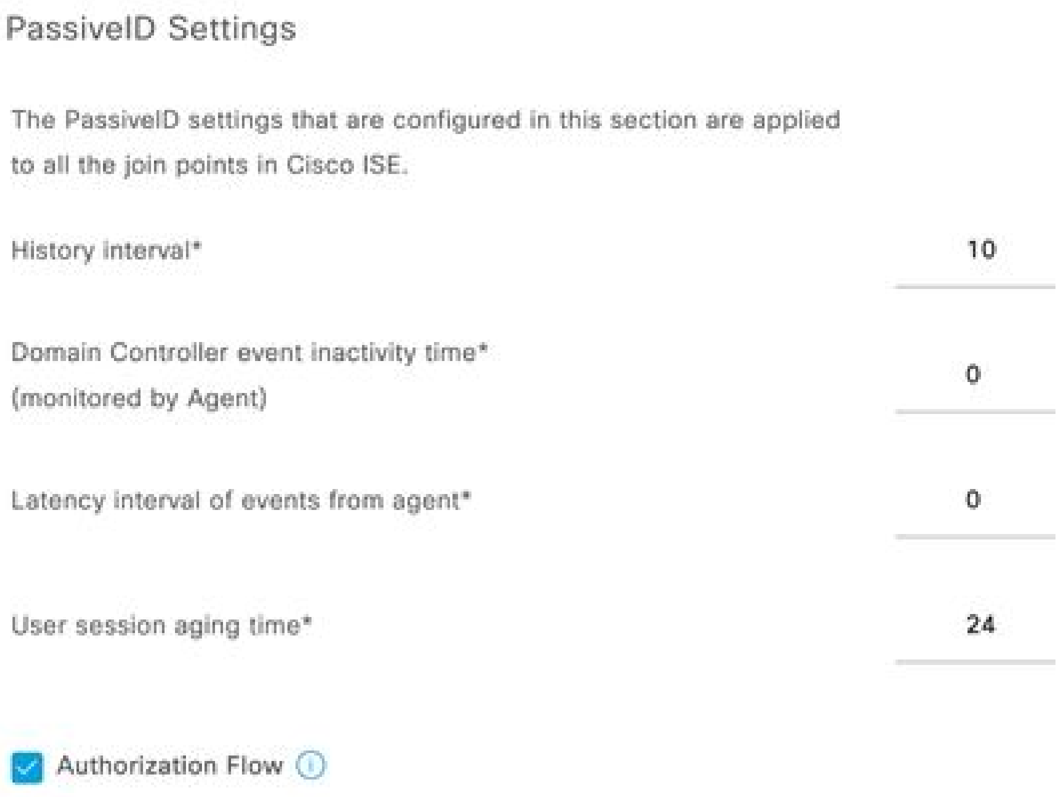
检索AD组



□	Name	S
□	aaamexrub.com/Users/Domain Admins	S
□	aaamexrub.com/Users/Domain Users	S
□	aaamexrub.com/Users/sponsors	S

检索的组

5.启用授权流程。导航到**高级设置**，并在**PassiveID设置**部分中选中**Authorization Flow**复选框。Click Save.



PassiveID Settings

The PassiveID settings that are configured in this section are applied to all the join points in Cisco ISE.

History interval* 10

Domain Controller event inactivity time* (monitored by Agent) 0

Latency interval of events from agent* 0

User session aging time* 24

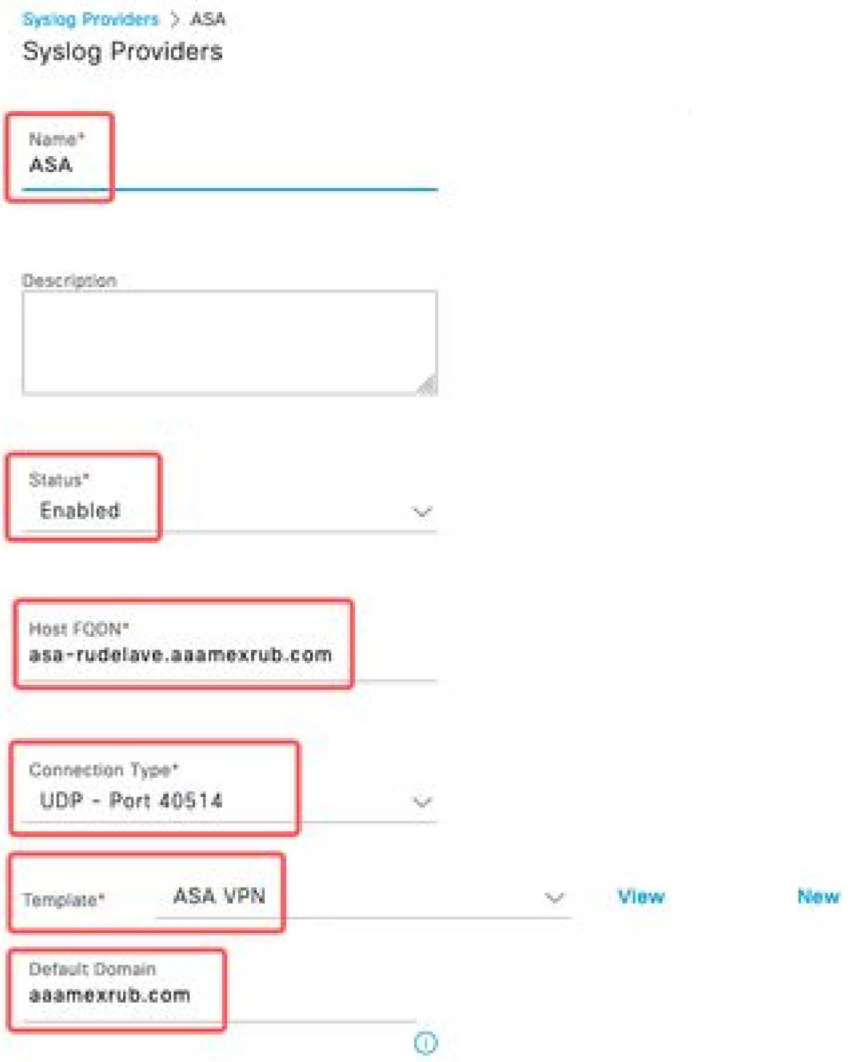
☑ Authorization Flow ⓘ

启用授权流

第三步：配置系统日志提供程序。

1. 导航到Work Centers > **PassiveID** > **Providers**，选择**Syslog Providers**，单击**Add**并填写信息。点击保存

   注意：在这种情况下，ISE从ASA中成功的VPN连接收到系统日志消息，但本文档不描述该配置。



Syslog Providers

Name*
ASA

Description

Status*
Enabled

Host FQDN*
asa-rudelave.aaamexrub.com

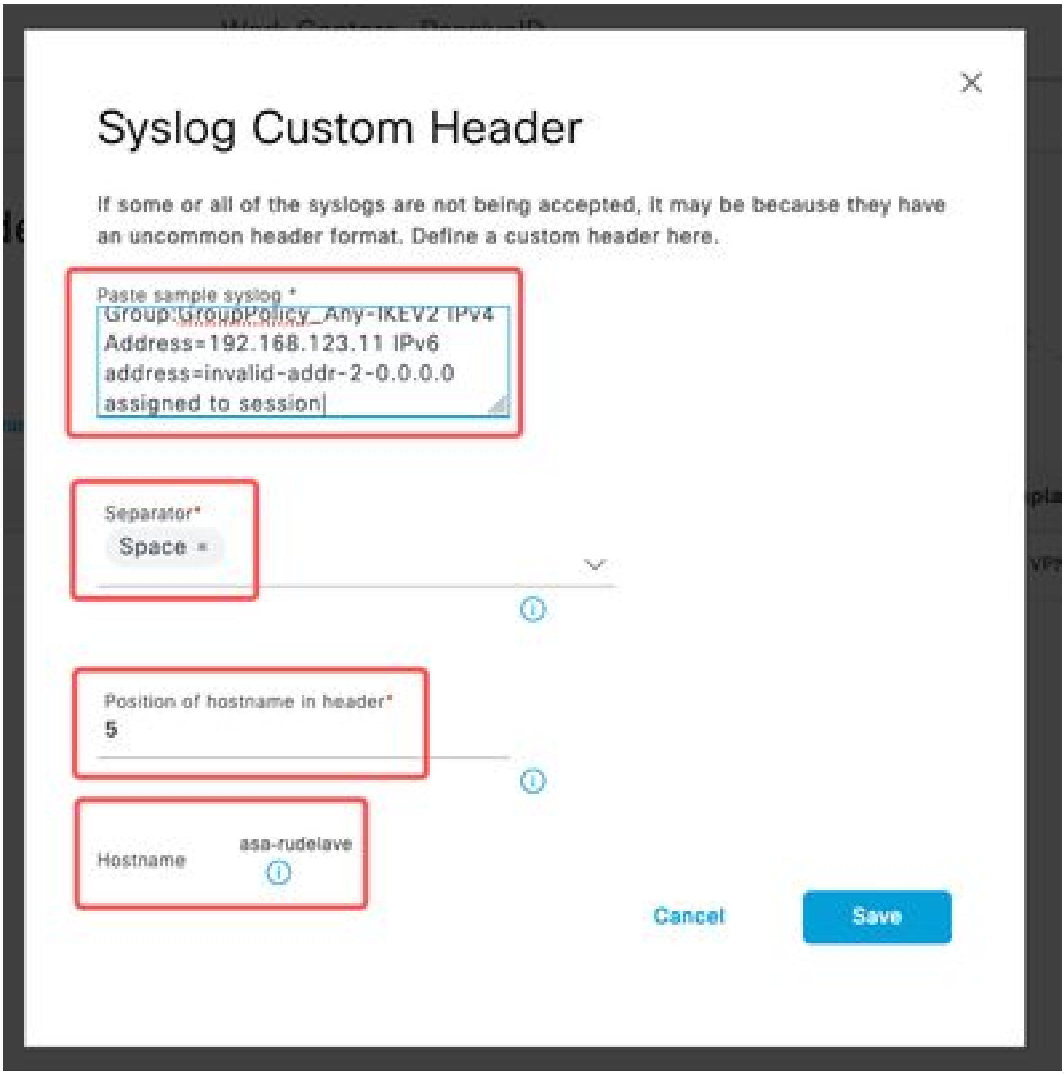
Connection Type*
UDP - Port 40514

Template*
ASA VPN

Default Domain
aaamexrub.com

配置系统日志提供程序

2. 单击**Custom Header**。粘贴示例系统日志并使用分隔符或选项卡查找设备主机名。如果正确，则显示主机名。点击保存



Syslog Custom Header

If some or all of the syslogs are not being accepted, it may be because they have an uncommon header format. Define a custom header here.

Paste sample syslog *

```
Group:GroupPolicy_Any-IKEV2 IPv4
Address=192.168.123.11 IPv6
address=invalid-addr-2-0.0.0.0
assigned to session
```

Separator*: Space

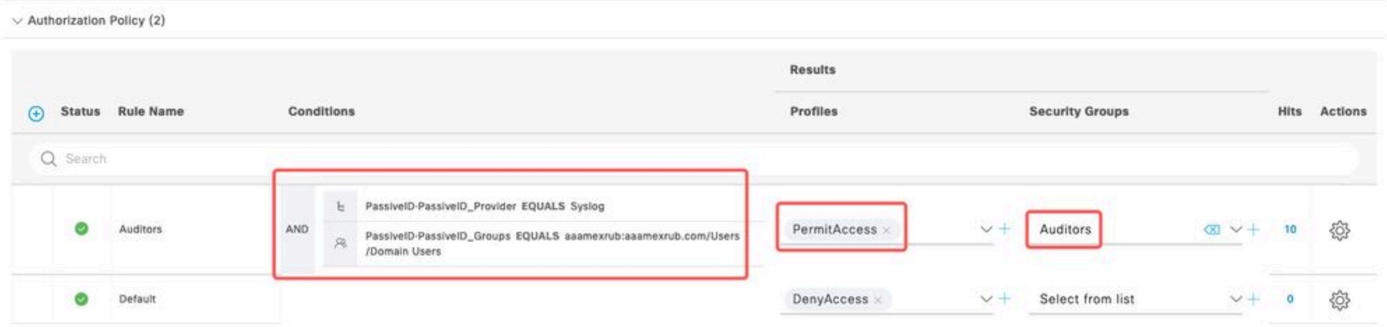
Position of hostname in header*: 5

Hostname: asa-rudelave

配置自定义信头

第四步：配置授权规则

1. 导航到**Policy** > **Policy Sets。** 在本例中，它使用默认策略。单击**Default**策略。在**授权策略**中，添加新规则。在PassiveID策略中，ISE包含所有提供程序。您可以将此组与PassiveID组组合。选择**Permit Access** as Profile，然后在**Security Groups**中选择需要的SGT。



Authorization Policy (2)

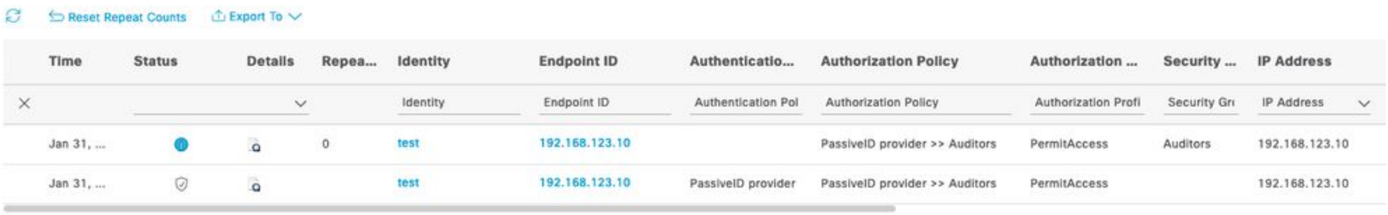
Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
●	Auditors	AND: PassiveID·PassiveID_Provider EQUALS Syslog PassiveID·PassiveID_Groups EQUALS aaamexrub:aaamexrub.com/Users/Domain Users	PermitAccess	Auditors	10	⚙
●	Default		DenyAccess	Select from list	0	⚙

配置授权规则

验证

ISE收到系统日志后，您可以检查Radius Live Logs查看授权流。导航到**操作** > **Radius** > **实时日志**。

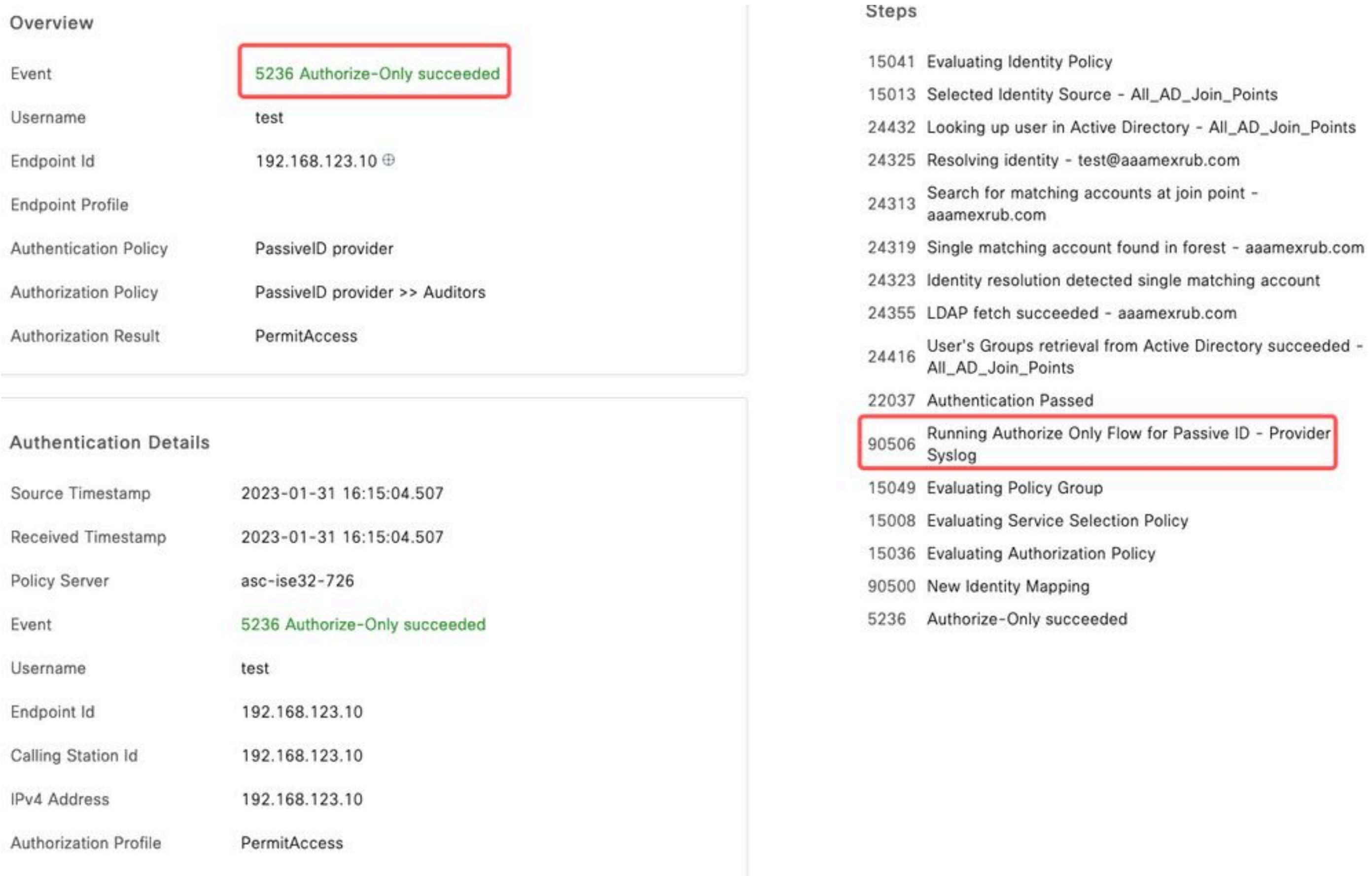
在日志中，您可以看到授权事件。此标签包含与其关联的用户名、授权策略和安全组标记。



Time	Status	Details	Repea...	Identity	Endpoint ID	Authenticatio...	Authorization Policy	Authorization ...	Security ...	IP Address
✕				Identity	Endpoint ID	Authentication Pol	Authorization Policy	Authorization Profi	Security Gr	IP Address
Jan 31, ...	●	🗎	0	test	192.168.123.10		PassiveID provider >> Auditors	PermitAccess	Auditors	192.168.123.10
Jan 31, ...	🛡	🗎		test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess		192.168.123.10

Radius实时日志

要检查更多详细信息，请点击**详细报告**。此处您可以看到评估策略以分配SGT的仅授权流程。



Overview

Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10 ⊕
Endpoint Profile	
Authentication Policy	PassiveID provider
Authorization Policy	PassiveID provider >> Auditors
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2023-01-31 16:15:04.507
Received Timestamp	2023-01-31 16:15:04.507
Policy Server	asc-ise32-726
Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Calling Station Id	192.168.123.10
IPv4 Address	192.168.123.10
Authorization Profile	PermitAccess

Steps

15041	Evaluating Identity Policy
15013	Selected Identity Source - All_AD_Join_Points
24432	Looking up user in Active Directory - All_AD_Join_Points
24325	Resolving identity - test@aaamexrub.com
24313	Search for matching accounts at join point - aaamexrub.com
24319	Single matching account found in forest - aaamexrub.com
24323	Identity resolution detected single matching account
24355	LDAP fetch succeeded - aaamexrub.com
24416	User's Groups retrieval from Active Directory succeeded - All_AD_Join_Points
22037	Authentication Passed
90506	Running Authorize Only Flow for Passive ID - Provider Syslog
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15036	Evaluating Authorization Policy
90500	New Identity Mapping
5236	Authorize-Only succeeded

Radius实时日志报告

故障排除

在本例中，它使用两个流：passiveID会话和授权流。要启用调试，请导航到**操作** > **故障排除** > **调试向导**> **调试日志配置**，然后选择ISE节点。

对于PassiveID，启用下一个组件到**DEBUG**级别：

- 被动ID

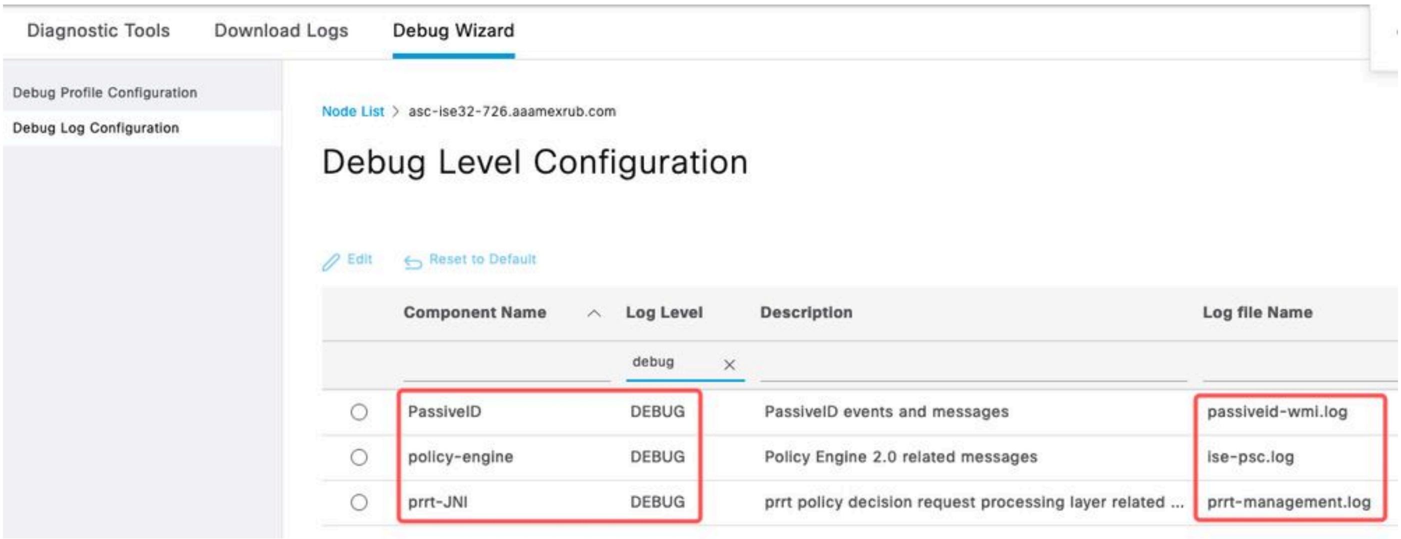
要根据被动ID提供程序检查日志以及要检查此方案的文件，您需要查看其他提供程序的**文件** passiveid-syslog.log:

- passiveid-agent.log
- passiveid-api.log
- passiveid-endpoint.log
- passiveid-span.log
- passiveid-wmilog

对于授权流，启用下一个组件到**DEBUG**级别：

- 策略引擎
- prrt-JNI

示例：



Debug Level Configuration

	Component Name	Log Level	Description	Log file Name
		debug		
○	PassiveID	DEBUG	PassiveID events and messages	passiveid-wmi.log
○	policy-engine	DEBUG	Policy Engine 2.0 related messages	ise-psc.log
○	prrt-JNI	DEBUG	prrt policy decision request processing layer related ...	prrt-management.log

启用调试

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。